UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

KENDRA HARPER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

NBI, INC.,

Defendant.

CASE NO. 24-cv-644

(JURY TRIAL DEMANDED)

AMENDED CLASS ACTION COMPLAINT[1]

Plaintiff Kendra Harper, individually and on behalf of all others similarly situated, makes the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to herself or her counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiff brings this action for legal and equitable remedies to redress and put a stop to Defendant **NBI, Inc.'s** practices of knowingly disclosing Plaintiff's and its other customers' identities, their subscription purchases, and the titles of the prerecorded video materials that they obtained to Meta Platforms, Inc. ("Meta"), formerly known as Facebook, Inc. ("Facebook"), in violation of the federal Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710.

[1] Plaintiff files this amended complaint within 21 days of service of a motion under Fed. R. Civ. P. 12(b), pursuant to Fed. R. Civ. P. 15(a)(1)(B).

2. Over the past two years, Defendant has systematically transmitted its customers' personally identifying subscription and video viewing information to Meta using a snippet of programming code called the "Meta Pixel," which Defendant chose to install on its nbi-sems.com website.

3. The information Defendant disclosed to Meta, via the Meta Pixel it installed on its website, includes a consumer's Facebook ID ("FID") coupled with a subscription purchase and the title of each of the specific videos that the consumer requested or obtained on Defendant's website. An FID is a unique sequence of numbers linked to the Meta profile belonging to that customer. The customer's Meta profile, in turn, publicly identifies the customer by name, and contains other personally identifying information about the customer as well. Entering "facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals the specific videos or subscriptions that a particular person requested or obtained from Defendant's website (hereinafter, "Private Viewing Information").

4. Defendant disclosed its customers' subscription purchases and Private Viewing Information to Meta without asking for, let alone obtaining, its customers' consent to these practices.

5. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information

concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), inter alia, liquidated damages in the amount of $2,500.00 per violation and equitable relief, *see id.* § 2710(c).

6. Accordingly, on behalf of herself and the putative Class members defined below, Plaintiff brings this Class Action Complaint against Defendant for intentionally and unlawfully disclosing their subscription and Personal Viewing Information to Meta.

PARTIES

I. Plaintiff Harper

7. Plaintiff Harper is a citizen and resident of Marion County, Indiana.

8. Plaintiff Harper is, and at all times relevant hereto was, a user of Meta.

9. Plaintiff Harper is a consumer of the video products and services offered on Defendant's nbi-sems.com website. One of the items she purchased from Defendant's website was a prerecorded video entitled "Negotiating Injury Claims: Secrets and Insider Tips." She purchased this prerecorded video in June 2024. In creating an account and purchasing videos, Plaintiff Harper provided her name, email address, payment information, and zip code.

10. When Plaintiff Harper used her account on Defendant's website to request and obtain the prerecorded video, Defendant disclosed to Meta Plaintiff Harper's FID, the specific title of the video she requested and obtained, and the URL where she requested access to and obtained the video. Defendant also disclosed to Meta information concerning the device Plaintiff Harper used to request and obtain the video.

11. At all relevant times, including when accessing Defendant's website and obtaining the prerecorded video material, Plaintiff Harper had a Meta account, a Meta profile, and an FID associated with such profile.

12. Plaintiff Harper has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Personal Viewing Information to Meta. In fact, Defendant has never even provided Plaintiff Harper with written notice of its practices of disclosing its customers' subscription purchases and Personal Viewing Information to third parties such as Meta.

13. Because Defendant disclosed Plaintiff Harper's Private Viewing Information—including her FID, the title of the prerecorded video she purchased from Defendant's website, and the URL where she requested access to and obtained the video on Defendant's website—to Meta during the applicable statutory period, Defendant violated Plaintiff Harper's rights under the VPPA and invaded her statutorily conferred interest in keeping such information, which bears on her personal affairs and concerns, private.

II. Defendant NBI, Inc.

14. Defendant is a domestic corporation that maintains its principal place of business at 1218 McCann Drive, Altoona, WI 54720.

15. Defendant operates an online digital library of video materials on its website nbi-sems.com, where it is engaged in the business of selling, *inter alia*, a wide variety of prerecorded video materials to consumers across the United States. On its website, Defendant sells approximately 2,400 prerecorded videos, 350 "live" webinars, 10 interactive elearning courses, 4 podcasts, and admission to 10 in-person events.[2]

JURISDICTION AND VENUE

16. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

17. Personal jurisdiction and venue are proper because Defendant maintains its

[2] https://nbi-sems.com/.

principle place of business in Altoona, Wisconsin, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

18. The VPPA prohibits companies like Defendant from knowingly disclosing to third parties like Facebook information that personally identifies consumers like Plaintiff as having viewed particular videos or other audio-visual products or services.

19. Specifically, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business…of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4), and defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

20. The VPPA's purpose is as apropos today as it was at the time of its enactment over 35 years ago. Leading up to the statute's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials, because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle

and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

21. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, it is the personal nature of such information, and the need to protect it from disclosure, that is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id*.

22. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[3]

23. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have

[3] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[4]

24. In this case, however, Defendant deprived Plaintiff and the unnamed Class members of that right by systematically (and surreptitiously) disclosing their subscription purchases and Personal Viewing Information to Facebook, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

25. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[5]

26. More than a decade later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a $26 billion dollar per year online advertising industry in the United States.[6]

27. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

---

[4] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, frank.senate.gov (Jan. 31, 2012).

[5] FCC, *The Information Marketplace* (Mar. 13, 2001), at 8-11, *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[6] *See Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[7]

28. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[8]

29. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[9]

30. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[10]

31. Recognizing the serious threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies

---

[7] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[8] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/.

[9] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of- consumer-database-marketing.html.

[10] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c.

collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[11]

32. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like NBI share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[12]

33. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[13] The FTC notes that "[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[14]

---

[11] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

[12] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

[13] *Id.*

[14] *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging* (August 10, 2000) (prepared statement of the FTC), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf.

34. Indeed, an entire black market exists where the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like Defendant's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[15]

35. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

II. Consumers Place Monetary Value on their Privacy and Consider Privacy Practices When Making Purchases

36. As the data aggregation industry has grown, so too have consumer concerns regarding their personal information.

37. A recent survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies whom they believe do not protect their privacy online.[16] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[17]

38. Thus, as consumer privacy concerns grow, consumers are increasingly incorporating privacy concerns and values into their purchasing decisions and companies viewed

---

[15] *Id.*

[16] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

[17] *Id.*

as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors.

39. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[18]

40. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[19]

41. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[20] As such, where a business offers customers a service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a service of less value than the service paid for.

III. Defendant Uses the Meta Pixel to Systematically Disclose its Customers' Subscription Purchases and Personal Viewing Information to Meta

42. As alleged below, when a consumer purchases a subscription to Defendant's

---

[18] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), *available at* http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[19] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on monetising privacy* (Feb. 27, 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy.

[20] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf ("It is obvious that people value online privacy.").

website, that purchase of the subscription, along with the consumer's FID, is communicated to Meta by way of the Meta Pixel. Additionally, when a consumer requests or obtains a specific video, the Meta Pixel technology on Defendant's website transmits the consumer's personally identifying information and detailed information concerning the specific interactions she or he takes on its website (including the consumer's Private Viewing Information revealing the specific videos that he or she requested or obtained) to Meta, without the consumer's consent, in clear violation of the VPPA.

A. The Meta Pixel

43. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta".[21] Since then, Meta has become the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birthdate, gender, and phone number or email.

44. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to allow them to track consumers' actions and report the actions back to Meta.

45. The Meta Pixel allows online-based companies like Defendant to build detailed profiles of their visitors by collecting information about how they interact with their websites, and to then use the collected information to service highly targeted advertising to them.

46. Additionally, a Meta Pixel installed on a company's website allows Meta "to match . . . website visitors to their respective [Meta] User accounts."[22] Meta is able to do this because it has assigned to each of its users an "FID" number: a unique and persistent identifier

---

21 Company Info, FACEBOOK, https://about.fb.com/company-info./.

22 https://developers.facebook.com/docs/meta-pixel/get-started.

that allows anyone to look up the user's unique Meta profile and thus identify the user by name.[23] Then, each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by the FID of the website's visitor. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after clearing browser history.

47. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site. Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."[24]

48. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.[25]

49. Meta's Business Tools Terms state that website operators may use Meta's Business Tools, including the Meta Pixel, to transmit the "Contact Information" and "Event Data" of their website visitors to Meta. The Tool Terms define "Contact Information" as "information that personally identifies individuals, such as names, email addresses, and phone numbers . . . ."[26]

50. Meta's Business Tools Terms state: "You instruct us to process the Contact Information solely to match the Contact Information against user IDs [e.g., FIDs] ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[27]

51. The Business Tools Terms define "Event Data" as, inter alia, "information that

---

[23] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

[24] Meta, "About Meta Pixel," available at https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[25] Meta, "Meta Business Tools Terms," available at https://www.facebook.com/legal/technology_terms.

[26] *Id*.

[27] *Id*.

you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products."[28]

52. Every transmission to Meta accomplished through the Meta Pixel includes at least two elements: (1) the website visitor's FID and (2) the URL of the webpage triggering the transmission.

53. Depending on the configuration of the Meta Pixel, the website may also send Event Data to Meta. Defendant has configured the Meta Pixel on its Website to send Event Data to Meta.

54. When website operators make transmissions to Meta through the Meta Pixel, none of the following categories of information are hashed or encrypted: the visitor's FID, the URL of the website, or the Event Data.

55. Every website operator installing the Meta Pixel must agree to the Meta Business Tools Terms. [29]

56. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

57. Simply put: if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able

[28] *Id.*

[29] *See id.*

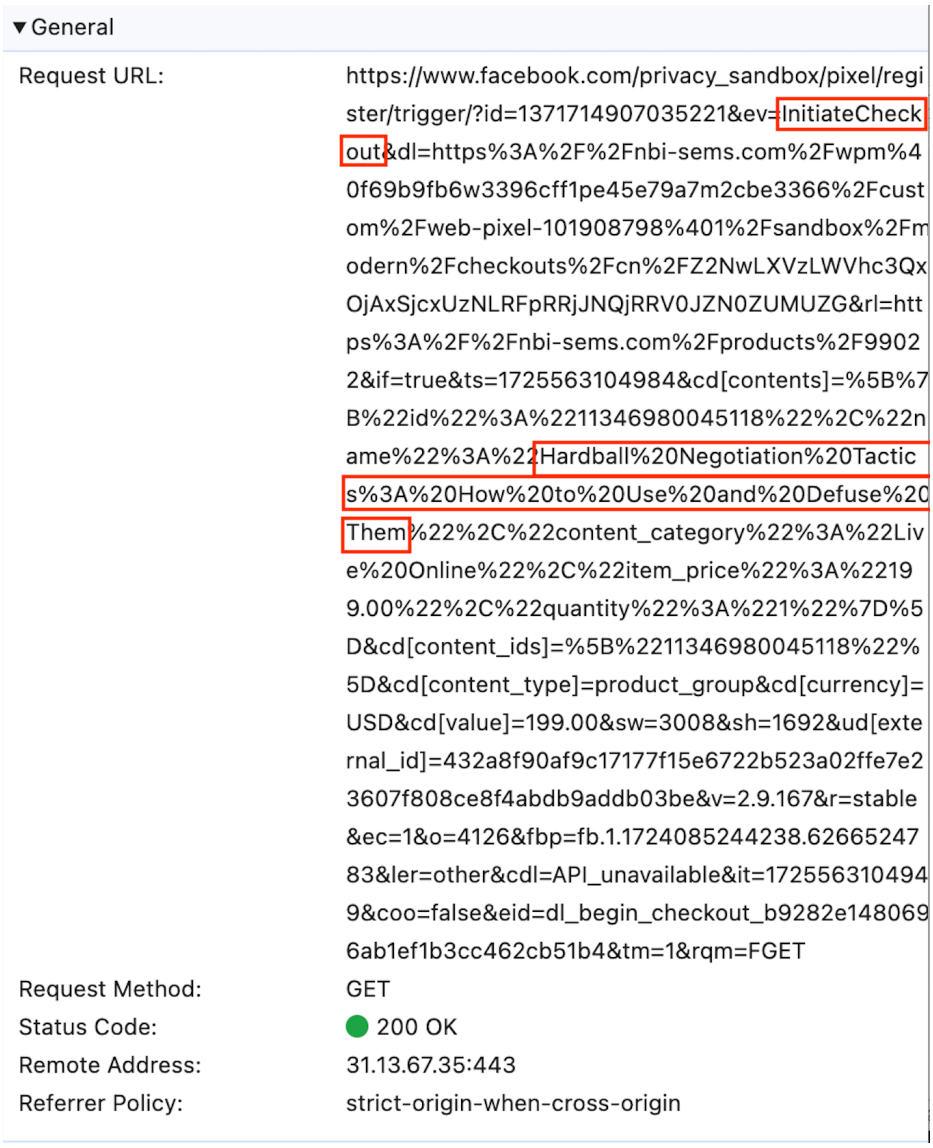
to "track[] the people and type of actions they take"[30] on the company's website, including the purchases they made, the items they spent time viewing, and, as relevant here, the specific video content that they requested or obtained on the website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit Its Customers' Subscription Purchases and Private Viewing Information to Meta

58. Defendant allows persons to become digital consumers of its various online-based video products and services by subscribing to or purchasing prerecorded videos on its website. To subscribe or obtain access to videos, the consumer must provide at least his or her name, email address, billing address, and credit- or debit-card (or other form of payment) information.

59. When a person requested or obtained a subscription to or videos from Defendant's website, Defendant used—and has used at all times relevant hereto—the Meta Pixel to disclose to Meta the unencrypted FID of the consumer and the subscription and specific videos that he or she requested or obtained from Defendant's website. To illustrate Defendant's disclosure, when a user clicked on a video title, added it to cart, and initiated checkout, Defendant transmitted to Meta through the pixel the user's FID, along with the title and URL of the video the person obtained or requested at each of those steps. The screenshot below shows the transmission of the title of the specific video requested to Meta when the user initated checkout on Defendant's website for the video entitled "Hardball Negotiation Tactics: How to Use and Defuse Them":

[30] https://www.facebook.com/business/goals/retargeting.



▼General

Request URL: https://www.facebook.com/privacy_sandbox/pixel/register/trigger/?id=1371714907035221&ev=InitiateCheckout&dl=https%3A%2F%2Fnbi-sems.com%2Fwpm%40f69b9fb6w3396cff1pe45e79a7m2cbe3366%2Fcustom%2Fweb-pixel-101908798%401%2Fsandbox%2Fmodern%2Fcheckouts%2Fcn%2FZ2NwLXVzLWVhc3QxOjAxSjcxUzNLRFpRRjJNQjRRV0JZN0ZUMUZG&rl=https%3A%2F%2Fnbi-sems.com%2Fproducts%2F990022&if=true&ts=1725563104984&cd[contents]=%5B%7B%22id%22%3A%2211346980045118%22%2C%22name%22%3A%22Hardball%20Negotiation%20Tactics%3A%20How%20to%20Use%20and%20Defuse%20Them%22%2C%22content_category%22%3A%22Live%20Online%22%2C%22item_price%22%3A%221999.00%22%2C%22quantity%22%3A%221%22%7D%5D&cd[content_ids]=%5B%2211346980045118%22%5D&cd[content_type]=product_group&cd[currency]=USD&cd[value]=199.00&sw=3008&sh=1692&ud[external_id]=432a8f90af9c17177f15e6722b523a02ffe7e23607f808ce8f4abdb9addb03be&v=2.9.167&r=stable&ec=1&o=4126&fbp=fb.1.1724085244238.6266524783&ler=other&cdl=API_unavailable&it=1725563104949&coo=false&eid=dl_begin_checkout_b9282e1480696ab1ef1b3cc462cb51b4&tm=1&rqm=FGET

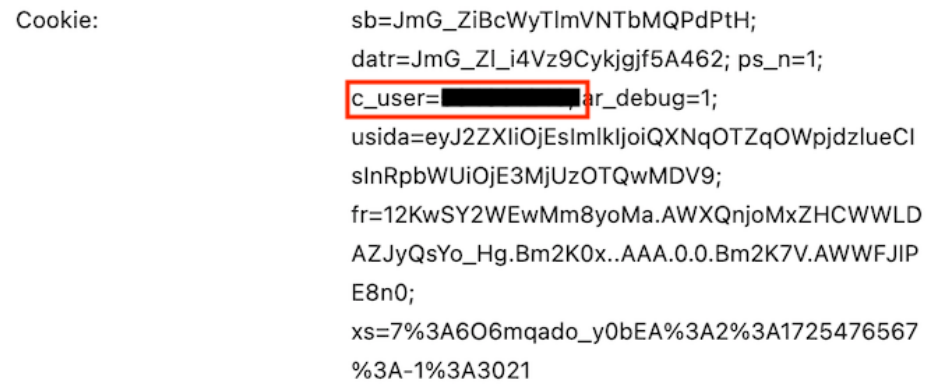
Request Method: GET

Status Code: 200 OK

Remote Address: 31.13.67.35:443

Referrer Policy: strict-origin-when-cross-origin

60. The transmissions at all stages of the purchase process were accompanied by the the user's FID, indentified by "c_user" in another screenshot from Defendant's website below:



Cookie: sb=JmG_ZiBcWyTlmVNTbMQPdPtH; datr=JmG_Zl_i4Vz9Cykjgjf5A462; ps_n=1; c_user=[redacted]ar_debug=1; usida=eyJ2ZXIiOjEsImlkIjoiQXNqOTZqOWpjdzlueCIsInRpbWUiOjE3MjUzOTQwMDV9; fr=12KwSY2WEwMm8yoMa.AWXQnjoMxZHCWWLDAZJyQsYo_Hg.Bm2K0x..AAA.0.0.Bm2K7V.AWWFJIPE8n0; xs=7%3A6O6mqado_y0bEA%3A2%3A1725476567%3A-1%3A3021

61. Once the user completed the purchase, the pixel sent notice of the purchase completion to Meta, along with the user's FID, notifying Meta that the user had purchased the video or subscription for which she or he had initiated checkout.

62. Defendant intentionally programmed its website (by following step-by-step instructions from Meta's website) to include a Meta Pixel that systematically transmits to Meta the FIDs of its customers, the specific titles of video products that each of them requested or obtained, and the purchase of a subscription in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta.

63. With only a person's FID and the video content name or URL that the person requested on Defendant's website—all of which Defendant knowingly provides to Meta—any ordinary person could learn the identity of the person to whom the FID corresponds and the specific video products or services that this person requested. This can be accomplished simply by accessing the URL www.facebook.com/[unencrypted FID].

64. Defendant's practices of disclosing consumers' purchases of subscriptions and Private Viewing Information to Meta continued unabated for the full duration of the time period relevant to this action. At all relevant times, whenever Plaintiff or another consumer purchased a subscription to Defendant's website or requested or obtained a particular video on Defendant's website, Defendant disclosed to Meta the subscription purchase or the specific video that was requested (including the URL where such video was accessed), along with the FID of the consumer who requested it, which, as discussed above, uniquely identifies the person.

65. At all relevant times, Defendant knew that the Meta Pixel disclosed its customers' subscription purchases and Private Viewing Information to Meta.

66. Defendant could easily have programmed its website so that none of its

customers' subscription purchases or detailed Private Viewing Information is disclosed to Meta. Instead, Defendant chose to program its website so that all of its customers' subscription purchases and detailed Private Viewing Information is sent to Meta *en masse*.

67. Prior to transmitting its customers' Private Viewing Information to Meta, Defendant failed to notify Plaintiff or any of its customers that it would do so, and neither Plaintiff nor any of its other customers have consented (in writing or otherwise) to these practices.

68. By intentionally disclosing to Meta Plaintiff's and its other customers' FIDs together with the subscription information and specific video content they each requested or obtained, without Plaintiff's or any of its other customers' consent to these practices, Defendant knowingly and systematically violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

69. Plaintiff seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, requested or obtained a subscription to Defendant's website or video content from Defendant's website while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

70. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

71. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include, but are not limited to: (a) whether Defendant knowingly disclosed Plaintiff's and Class

members' subscription purchases and Private Viewing Information to Meta; (b) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; (c) whether Defendant should be enjoined from disclosing Plaintiff's and Class members' subscription and Private Viewing Information to Meta; and (d) whether Plaintiff and Class members are entitled to statutory damages for the aforementioned violations.

72. The named Plaintiff's claims are typical of the claims of the Class in that the named Plaintiff and the Class members suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their subscription and Private Purchase Information to Meta.

73. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of Class members.

74. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer

management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION

(Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710)

75. Plaintiff repeats the allegations asserted in the preceding paragraphs as if fully set forth herein.

76. Plaintiff brings her claim individually and on behalf of the putative Class Members against Defendant.

77. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

78. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of delivering audiovisual materials that are similar to prerecorded video cassette tapes and those sales affect interstate or foreign commerce.

79. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiff and Class members, having purchased subscriptions or requested or obtained videos from

Defendant's website, are consumers of Defendant's services or video content. Thus, Plaintiff and Class members are "consumers" as defined in 18 U.S.C. § 2710(a)(1).

80. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." Defendant knowingly disclosed Plaintiff's and Class members' subscription purchases and Private Viewing Information to Meta in the manner alleged herein. The subscription and Private Viewing Information that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because the transmitted information identified Plaintiff and each Class member to Meta as an individual who purchased a subscription or requested or obtained video content, including the specific video materials requested or obtained from Defendant's website.

81. Defendant never obtained informed, written consent from Plaintiff or any Class member to disclose their Private Viewing Information to Meta or any other third party. More specifically, Defendant never obtained from Plaintiff or any Class member informed, written consent in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; Defendant never obtained from Plaintiff or any Class member informed, written consent that, at the election of the consumer, was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner; and Defendant never provided an opportunity, in a clear and conspicuous manner, for Plaintiff or any Class member to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

82. Defendant knowingly disclosed such information to Meta because Defendant

intentionally installed and programmed the Meta Pixel code on its website, knowing that such code would transmit to Meta the subscription purchases and video titles requested by its customers, along with the customers' unique identifiers (including FIDs), when consumers subscribed to or requested or obtained videos from its website.

83. By disclosing Plaintiff's and Class members' subscription purchases and Private Viewing Information, Defendant violated their statutorily protected right to privacy in the videos they requested or obtained from Defendant. 18 U.S.C. § 2710(c).

84. As a result of these violations, Defendant is liable to Plaintiff and Class members for damages and other relief as provided by the VPPA.

85. On behalf of herself and all members of the Class, Plaintiff seeks to enjoin Defendant's future disclosures of its consumers' subscription purchases and Private Viewing Information; liquidated damages in the amount of $2,500 per violation of the VPPA; reasonable attorneys' fees and costs; and all other preliminary or equitable relief the Court deems appropriate. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant **NBI, Inc.,** as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order declaring that Defendant's conduct as described herein violated the VPPA;

C. For an order finding in favor of Plaintiff and the Class and against Defendant on all counts asserted herein;

D. For an award of $2,500.00 to the Plaintiff and each Class member, as provided by the VPPA, 18 U.S.C. § 2710(c);

E. For an order permanently enjoining Defendant from disclosing the Private Viewing Information of its customers to third parties in violation of the VPPA.

F. For prejudgment interest on all amounts awarded; and

G. For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Class under Rule 23 and 18 U.S.C. § 2710(c).

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: November 5, 2024

Respectfully submitted,

HEDIN LLP

/s/ Frank S. Hedin

FRANK S. HEDIN
JULIE E. HOLT
HEDIN LLP
1395 BRICKELL AVE., SUITE 610
MIAMI, FLORIDA 33131-3302
TELEPHONE: (305) 357-2107
FACSIMILE: (305) 200-8801
FHEDIN@HEDINLLP.COM
JHOLT@HEDINLLP.COM

Attorneys for Plaintiff and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on November 5, 2024, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will provide electronic notification of such filing to all parties of record and served a copy via email on Defendant's retained counsel.

/s/ Frank S. Hedin